Pace Law Review

Volume 37
Issue 1 *Fall 2016*

Article 10

September 2016

Upholding Citizens' Privacy in the Use of Stingray Technology: Is New York Behind?

Samantha Hazen
Elisabeth Haub School of Law at Pace University, shazen@law.pace.edu

Upholding Citizens' Privacy in the Use of Stingray Technology: Is New York Behind?

Samantha Hazen*

I. Introduction

The word "Stingray" likely does not resonate with citizens as something other than a marine animal. But in the realm of privacy, the word carries a much different (perhaps more dangerous) meaning. Stingray devices belong to a family of cell-site simulators that track a cell phone user's location.[1] Federal, state, and local agencies purchase these devices and use them during investigations to pinpoint a suspect's location.[2] The devices—which are the size of a briefcase—act as cell phone towers and gather enough identifying information to locate the suspect.[3]

Despite its obvious advantage of promoting security, the technology also plays a controversial role: detecting and tracking cell phones besides the suspect's.[4] The idea of tracking multiple cell phones in a given region raises privacy

* J.D. Candidate, May 2017, Elisabeth Haub School of Law at Pace University. Seeing my work in print is a very humbling experience, and I owe this opportunity to *Pace Law Review*. I would like to thank Professor David N. Dorfman and Professor Bennett L. Gershman for providing guidance and for listening to my ideas in this ever-developing field. I am forever thankful to those who have stuck by my side, not only as I worked on this paper, but throughout law school as well.

1. Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 1:00 PM), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

2. *Stingray Tracking Devices*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices (last visited Nov. 12, 2015).

3. *Legislative Memo: In Support of a Warrant Requirement for the Use of Stingrays*, N.Y. CIV. LIBERTIES UNION (Aug. 24, 2015), http://www.nyclu.org/content/support-of-warrant-requirement-use-of-stingrays [hereinafter *Legislative Memo*].

4. *Id.*

concerns and other questions.[5] For example, what do agencies do with the location information? Do they delete the information, or store it indefinitely? Should bystanders be concerned that agencies will access their calls and text messages? The United States Department of Justice [hereinafter "DOJ"] acknowledged these concerns and introduced a new policy on September 3, 2015 for federal agencies' use of the technology.[6]

The DOJ's new policy prioritizes "transparency and accountability," which ultimately "increase[s] privacy" for citizens.[7] In the past, federal law enforcement agencies simply needed "legal authorization[]" to use cell-site simulators under the federal Pen Register Statute.[8] Now, federal agents must apply for a "search warrant supported by probable cause" before using the devices.[9] The warrant requirement is waived, however, in exigent or exceptional circumstances.[10] The DOJ also revealed that it will delete data as soon as the suspect is found, and it will not collect data such as text messages and emails.[11] In its policy, the DOJ explained that cell-site

5. *See* Julia Edwards, *Justice Department Tightens Cellphone Tracking Rules*, REUTERS (Sept. 3, 2015, 9:12 PM), http://www.reuters.com/article/2015/09/04/us-usa-justice-mobilephone-idUSKCN0R32B420150904#2GlQ782uO0Rs9JBv.97.

6. *Id.*

7. *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, U.S. DEP'T. OF JUST. (Sept. 3, 2015), http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [hereinafter *Justice Department Announces*].

8. *Id. See Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, U.S. DEP'T. OF JUST. (Sept. 3, 2015), https://www.justice.gov/opa/file/767321/download [hereinafter *Department of Justice Policy Guidance*].

9. *Justice Department Announces*, *supra* note 7.

10. *Id.* Exigent circumstances exist when "the needs of law enforcement [are] so compelling that the warrantless search is objectively reasonable under the Fourth Amendment." Mincey v. Arizona, 437 U.S. 385, 394 (1978). *See* Missouri v. McNeely, 133 S. Ct. 1552, 1559 (2013) (citations omitted) (holding that officers may sometimes conduct a warrantless search "to prevent the imminent destruction of justice"); Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (finding exigent circumstances when officers tend to "persons who are seriously injured or threatened with such injury"); United States v. Santana, 427 U.S. 38, 42-43 (1976) (holding that officers did not need a warrant to re-enter the suspect's home during a "chase").

11. *Justice Department Announces*, *supra* note 7.

simulators are not to be confused with a global-positioning system (GPS) because cell-site simulators "do not obtain or download any location information from the device or its applications."[12] The DOJ also stated that cell-site simulators "must be configured as pen registers" and accord with relevant statutory provisions, including 18 U.S.C. § 3127.[13] Finally, the DOJ emphasized that the policy "is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law . . . [or] any right of review in an administrative, judicial, or any other proceeding."[14]

One month later, the United States Department of Homeland Security [hereinafter "DHS"] followed the DOJ's lead and implemented a probable cause requirement for the use of cell-site simulators.[15] Similar to the DOJ's policy, the DHS will not require its agents to seek warrants supported by probable cause in exigent or exceptional circumstances.[16] The

12. *Department of Justice Policy Guidance*, *supra* note 8, at 3. *But see infra* note 132. Despite the DOJ's distinction, the United States Supreme Court in *United States v. Jones* still regarded the use of GPS as a search requiring a warrant under the Fourth Amendment. *See generally* United States v. Jones, 132 S. Ct. 945, 949 (2012).

13. *Department of Justice Policy Guidance*, *supra* note 8, at 2. For a discussion of pen register use and the Fourth Amendment, see Smith v. Maryland, 442 U.S. 735 (1979) (holding that "[t]he installation and use of a pen register. . . was not a 'search,' and no warrant was required"). Only seven years after *Smith*, however, Congress limited pen register use through various statutes, indicating that pen registers should not go unregulated. JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: INVESTIGATING CRIME 112 n.3 (5th ed. 2013).

14. *Department of Justice Policy Guidance*, *supra* note 8, at 2 n.2.

15. *Department Policy Regarding the Use of Cell-Site Simulator Technology*, U.S. DEP'T OF HOMELAND SEC. (Oct. 19, 2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf [hereinafter *Department Policy*].

16. *Id.* See *supra* note 10 for examples of exigent circumstances. The DHS also lists the following: "the need to protect human life or avert serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice." *Id.* For exceptional circumstances, including "potential uses of the technology in furtherance of protective duties pursuant to 18 U.S.C. § 3056 and 18 U.S.C. § 3056A," agents are required to "obtain approval from executive-level personnel at the Component's [DHS's]

DHS makes clear, however, that its agents must still obtain judicial approval pursuant to the Pen Register Statute and must comply with the statute's emergency provisions.[17] When submitting applications to the court, DHS agents "must disclose appropriately and accurately the underlying purpose and activities for which an order or authorization is sought."[18] The agents must also explain, with specificity, their desired technique, their goal in using the technology, any disruptions in cellular service, and their method of collecting and deleting data.[19] The new policy echoes the DOJ's policy by affording privacy to citizens and assuring their civil liberties are not violated through the use of advanced technology.[20]

The United States Internal Revenue Service [hereinafter "IRS"] became the third federal agency to rethink its cell-site simulator policy before the end of 2015.[21] John A. Koskinen, IRS Commissioner, provided details about the agency's cell-site simulator use, which began in 2011.[22] In a letter to United States Senator Ron Wyden, Koskinen wrote that the IRS's Criminal Investigation division [hereinafter "IRS-CI"] currently owns one simulator, but is actively seeking another.[23] The IRS-CI first used its simulator during "early 2012" and has since tracked thirty-seven cell phones "in support of eleven federal grand jury investigations."[24] Koskinen wrote that the agency also used the simulator during a Drug Enforcement Agency [hereinafter "DEA"] action.[25] In sum, the DOJ's September 2015 policy spurred change within the IRS.[26] The agency decided that it would "mirror the DOJ policy's

headquarters and the relevant U.S. Attorney, who coordinates approval within the Department of Justice." *Id.*

17. *Id.* *See* 18 U.S.C. §§ 3121, 3125 (2012).

18. *Department Policy*, *supra* note 15.

19. *Id.*

20. *Id.*

21. Letter from John A. Koskinen, IRS Comm'r, to Ron Wyden, U.S Senator (Nov. 25, 2015), http://www.wyden.senate.gov/download/?id=6c9cd25c-28d1-4cda-9199-04a15c0b5d33&download=1.

22. *Id.*

23. *Id.*

24. *Id.*

25. *Id.*

26. Letter from John A. Koskinen, *supra* note 21.

requirement[s]" and draft a new policy by November 30, 2015.[27]

While these new policies represent a big step toward privacy and transparency in information-gathering, they do not extend as far as many would prefer. In fact, the DOJ's policy does *not* apply to state and local law enforcement agencies, unless the DOJ uses the devices "in support of" these other agencies.[28] The DHS's new policy, too, only applies to the actions of its own agents, though the DHS recognizes that its agents often work with state and local governments.[29]

According to a map created by the American Civil Liberties Union [hereinafter "ACLU"], "57 agencies in 22 states and the District of Columbia" use Stingray technology.[30] The ACLU's map differentiates among states that use cell-site simulators at the local level, the state level, or both. [31] Some of these states, including Washington and Virginia, have a warrant requirement, but many do not.[32] Most recently, in October 2015, California implemented a warrant requirement for access to "electronic communication information," which includes "location of the sender or recipients at any point during the communication."[33] New York, which uses Stingrays at the local and state levels,[34] does not have a Stingray policy that requires warrants supported by probable cause.[35]

27. *Id.*

28. Ellen Nakashima, *Justice Department: Agencies Need Warrant to Use Cellphone Trackers*, WASH. POST (Sept. 3, 2015), https://www.washingtonpost.com/world/national-security/justice-department-agencies-will-have-to-obtain-warrant-before-using-cellphone-surveillance-technology/2015/09/03/08e44b70-5255-11e5-933e-7d06c647a395_story.html; *Department of Justice Policy Guidance*, *supra* note 8, at 6.

29. *Department Policy*, *supra* note 15.

30. *Stingray Tracking Devices: Who's Got Them*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them#agencies (last visited Oct. 20, 2016) [hereinafter *Stingray Tracking Devices*].

31. *Id.*

32. Cyrus Farivar, *Cops Must Now Get a Warrant to Use Stingrays in Washington State*, ARS TECHNICA (May 12, 2015, 9:49 AM), http://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/. *See also* WASH. REV. CODE § 9.73.270 (2015); VA. CODE ANN. § 19.2-56.2 (2012).

33. S.B. 178, 2015-2016 Reg. Sess. (Cal. 2015).

34. *Stingray Tracking Devices*, *supra* note 30.

35. *Memorandum: Warrant Requirement for the Use of Stingrays in New*

New York's standard marks a striking distinction. This Comment will argue that New York should follow the federal agencies' and states' leads by imposing a warrant requirement supported by probable cause on local and state agencies that wish to use Stingray technology in their investigations. The first section will explore Stingray technology and how it works. The second section will frame the issue and describe New York's current standard. The third section will discuss the judicial response to the issue and how New York courts seem to place the burden of upholding privacy on the citizen, instead of the government. The third section will also discuss a possible shift in New York courts' stance on privacy, examining a recent dispute in Erie County that involved unauthorized Stingray use. The fourth section will discuss the legislative response to the issue, which consists of two state bills and a federal bill that could change New York's policy. The fifth and final section will argue why New York should adopt a warrant requirement supported by probable cause.

II. What is a Stingray?

As mentioned above, "Stingray" is just one name for a collection of cell-site simulators.[36] Cell-site simulators, also called International Mobile Subscriber Identity (IMSI) catchers, "trick . . . phones nearby into connecting to the device in order to log the IMSI number of mobile phones in the area or capture the content of communications."[37] Other names for the tracking technology include Gossamer and triggerfish.[38] The

York, N.Y. CIV. LIBERTIES UNION (Aug. 2015), http://www.nyclu.org/files/memo_stingrayuse_NY_201508_final.pdf [hereinafter *Memorandum: Warrant Requirement*].

36. *Stingray Tracking Devices*, *supra* note 30; Harris Corporation, a Florida-based company, manufactures Stingrays and other "surveillance technologies" used by government agencies. *See* Gallagher, *supra* note 1.

37. *Cell-Site Simulators: Frequently Asked Questions*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/sls/tech/cell-site-simulators/faq#faq-How-do-law-enforcement-agencies-use-cell-site-simulators? (last visited Oct. 20, 2016) [hereinafter ELECTRONIC FRONTIER FOUND.].

38. Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, WIRED (Oct. 28, 2015, 3:00 PM), http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/.

name "Stingray" dominates, however, because its manufacturer, Harris Corporation, reportedly has an exclusive contract with the United States.[39] According to technology publication *Ars Technica*, Harris' products "provide capabilities that authorities claim other companies do not offer."[40]

Federal, state, and local agencies may purchase cell-site simulators from Harris Corporation or various other outlets, including Rayzone and Atos.[41] Once purchased, Stingray installation should not be an issue, as Stingrays "can be covertly set up virtually anywhere."[42] Stingrays use a stronger signal than mobile service towers to force cell phones in the area to register with the Stingray instead.[43] A Stingray's range spans approximately 1,000 feet, but varies with antenna size and other specifications.[44] While it is not definitively clear, some sources specify that a cell phone must be powered on for a Stingray to track it.[45]

Once a cell phone registers, the Stingray can obtain the phone's unique ID and pinpoint its exact location—even inside an office or residence.[46] The officer or agency using the device can then use a computer connected to the Stingray to access the data.[47] Aside from location-tracking, Stingrays also have the capability to reveal the "content of communications."[48] The DOJ asserts, however, that its agents cannot use Stingrays to intercept communications, including "emails, texts, contact lists and images."[49]

Stingray use seems to have taken off in the new millennium.[50] According to *Ars Technica*, "[t]rademark records

39. Gallagher, *supra* note 1.
40. *Id.*
41. ELECTRONIC FRONTIER FOUND., *supra* note 37.
42. Gallagher, *supra* note 1.
43. Zetter, *supra* note 38.
44. ELECTRONIC FRONTIER FOUND., *supra* note 37.
45. *Id.*
46. Zetter, *supra* note 38.
47. Matthew Keys, *Exclusive: Stingray Maker Asked FCC to Block Release of Spy Gear Manual*, THEBLOT.COM (Mar. 26, 2015), http://www.theblot.com/exclusive-stingray-maker-asked-fcc-to-block-release-of-spy-gear-manual-7739514.
48. Gallagher, *supra* note 1.
49. *Justice Department Announces*, *supra* note 7.
50. *See* Gallagher, *supra* note 1.

show that a registration for the Stingray was first filed in August 2001."[51] Since then, government agencies have frequently purchased the device, which costs approximately $70,000 for the original or $135,000 for an updated version.[52] *Ars Technica* estimates that cell-site simulator manufacturers have made millions on the product since the early 2000s.[53]

Much controversy surrounds the use of Stingray technology.[54] News outlets and other sources frequently use one word to describe the controversy: secrecy.[55] For example, citizens may believe that agencies only use the technology for national security purposes, but may not know that they also use it for local, criminal investigations.[56] Citizens are not the only ones unaware of the scope of Stingray use; the *courts* have also been shielded from Stingray use in local investigations.[57] For example, beginning in 2010, officers in Erie County, New York used Stingrays forty-six times without a court order or a warrant.[58]

The secrecy stems from non-disclosure agreements between cell-site simulator manufacturers, such as Harris Corporation, and local or state agencies.[59] One example of a non-disclosure agreement between the City of Tucson, Arizona and Harris reads:

> The City of Tucson shall not discuss, publish, release or disclose any information pertaining to products covered under this [non-disclosure agreement] to any third party individual, corporation . . . or other governmental entity

51. *Id.*

52. *Id.*

53. *Id.*

54. *See* Kim Zetter, *NY Cops Used 'Stingray' Spy Tool 46 Times Without Warrant*, WIRED (Apr. 7, 2015, 5:08 PM), http://www.wired.com/2015/04/ny-cops-used-stingray-spy-tool-46-times-without-warrant/.

55. ELECTRONIC FRONTIER FOUND., *supra* note 37.

56. *Id.*

57. *See* Zetter, *supra* note 54.

58. *Id.*

59. Complaint & Application for Order to Show Cause at 3, Hodai v. City of Tucson, 2014 Ariz. Super. LEXIS 2158 (Ariz. Sup. Ct. Dec. 11, 2014) (No. C20141225).

> without the prior written consent of Harris . . . in the event that the city receives a Public Records request from a third party relating to any Protected Product, or other information Harris deems confidential, the City will notify Harris of such a request and allow Harris to challenge any such request in court.[60]

Lawyers and journalists around the country wish to uncover and expose the details of agencies' Stingray use so that citizens are fully aware of the technology's capabilities. That endeavor becomes more difficult, however, in states like New York, where local and state agencies can use Stingrays without obtaining a warrant supported by probable cause.[61]

III. New York's Current Standard: No Warrant Requirement

Although the DOJ has made significant steps toward privacy through its September 2015 policy announcement, the policy falls short because it does not affect the states.[62] Some states, however, either have cell-site simulator policies or have recently clarified their stances. For example, the Pennsylvania State Police (PSP) has a fact sheet that discloses its ownership of a cell-site simulator and explains how it is used.[63] In Raleigh, North Carolina, police department spokesperson Jim Sughrue has stated that "departmental use of the [cell-site simulator] technology complies with state and federal

60. *Id.* at 3-4.

61. *Legislative Memo*, *supra* note 3.

62. *ACLU Comment on New Justice Department Guidelines for Secretive Stingray Surveillance Devices*, AM. CIV. LIBERTIES UNION (Sept. 3, 2015), https://www.aclu.org/news/aclu-comment-new-justice-department-guidelines-secretive-stingray-surveillance-devices.

63. *FAQ's on Cell Site Simulators*, PA. STATE POLICE, http://www.psp.pa.gov/public-safety/Documents/FAQ%20CellSiteSimulators%202015%20revision3.pdf (last visited Jan. 22, 2016). The Pennsylvania State Police seeks a court order "approved and signed by a Judge in either the Court of Common Pleas or the PA Superior Court" before using the device, except in exigent circumstances. *Id.*

requirements."[64] Sughrue, however, did not go into further detail.[65]

To date, New York does not have a Stingray policy that requires a warrant supported by probable cause.[66] The New York Civil Liberties Union [hereinafter "NYCLU"], a non-profit civil rights group founded in 1951, does not think warrantless use of Stingrays in New York should continue, urging the state to take a stance.[67] On October 30, 2015 the New York City Police Department's [hereinafter "NYPD"] Legal Bureau responded to a Freedom of Information Law (FOIL) request from NYCLU, confirming its ownership and use of cell-site simulators without a warrant.[68] This was the first time the NYPD publicly acknowledged its use of Stingrays, showing that it had used the technology more than 1,000 times between 2008 and May 2015.[69]

In its response, the NYPD stated that it does not have a written cell-site simulator policy, but it does have a two-page non-disclosure agreement with Harris Corporation.[70] The NYPD also stated that it follows New York's Criminal Procedure Law § 705 before using cell-site simulators.[71] The Criminal Procedure Law does not specifically reference Stingrays or other cell-site simulators, but § 705.10 does discuss the use of pen registers and trap and trace devices,[72] which are instruments that record metadata.[73] Metadata is a

64. *Raleigh, Durham Police Using Device that Tracks Cellphone Data*, WRAL (July 28, 2014), http://www.wral.com/raleigh-durham-police-using-device-that-tracks-cellphone-data/13847158/.

65. *Id.*

66. *Memorandum: Warrant Requirement*, *supra* note 35.

67. *Id.*

68. Letter from Richard Mantellino, Lieutenant, Records Access Officer, NYPD, to Mariko Hirose, N.Y. Civil Liberties Union (Oct. 30, 2015), http://www.nyclu.org/files/releases/NYPD%20original%20FOIL%20response%20Stingrays.pdf.

69. *NYPD Has Used Stingrays More Than 1,000 Times Since 2008*, N.Y. CIV. LIBERTIES UNION (Feb. 11, 2016), http://www.nyclu.org/news/nypd-has-used-stingrays-more-1000-times-2008.

70. Letter from Richard Mantellino, *supra* note 68.

71. *Id.*

72. N.Y. CRIM. PROC. LAW § 705.10 (1988).

73. OFF. OF THE INSPECTOR GEN., U.S. DEP'T. OF JUST., A REVIEW OF THE FBI'S USE OF PEN REGISTER AND TRAP AND TRACE DEVICES UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT IN 2007 THROUGH 2009 1 (2015),

collection of "telephone numbers, e-mail addresses, and other dialing, routing, addressing, or signaling information that it is transmitted by instruments or facilities . . . that carry wire or electronic communications."[74] Similar to the cell-site simulator policy, the DOJ states that pen register and trap and trace devices do not record the "contents of communications."[75] Under § 705.10, an agency need only obtain a court order supported by "reasonable suspicion" to use a pen register or trap and trace device.[76] In the Editors' Notes, commentator Peter Preiser notes the lower burden of proof and that the "probable cause" standard is "constitutionally and statutorily required for search and electronic eavesdropping warrants."[77] Finally, the NYPD listed situations where it did not apply for a court order before it used a cell-site simulator because of "compellingly exigent circumstances."[78] The examples, spanning from 2008 through May 21, 2015, include kidnaping, robbery, homicide, missing person, and stalking.[79]

Less than three months before the NYPD's response, the NYCLU published a memorandum that analyzed New York's eavesdropping laws, concluding that New York should require warrants.[80] The memorandum first mentions the irony of warrantless searches in New York in light of the fact that New York offers greater eavesdropping protection to citizens than the United States Constitution does.[81] In particular, the NYCLU honed in on New York Penal Law § 250.05, the state's eavesdropping law.[82] The memorandum explained that it is unlawful to eavesdrop without a warrant issued under § 700 or a court order issued under § 705.[83] The NYCLU reads the

https://oig.justice.gov/reports/2015/o1506.pdf.

74. *Id.*

75. *Id.*

76. § 705.10.

77. *Id. See also Memorandum: Warrant Requirement*, *supra* note 35, which discusses the eavesdropping warrant requirement.

78. Letter from Richard Mantellino, *supra* note 68.

79. *Id.*

80. *Memorandum: Warrant Requirement, supra* note 35.

81. *Id.* at 2. ("New York's criminal prohibition on eavesdropping is broader than its federal counterpart." *Id.*).

82. *Id. See* N.Y. PENAL LAW § 250.05 (McKinney 2016).

83. *Id.*

eavesdropping law to regulate Stingrays "even when it is not being used to eavesdrop on phone conversations and messages" because of further definitions found in § 250.00.[84] First, § 250.00(6) defines "intercepting or accessing of an electronic communication" as "*intentional acquiring*, *receiving, collecting*, overhearing, or recording of an electronic communication, *without the consent of the sender or intended receiver*, by *means of any instrument,* device or equipment. . . ."[85] Next, "electronic communication" is "any transfer of signs, signals, writing . . . or intelligence of any nature. . . ."[86] But, as the memorandum points out, there are exceptions to § 250.00(5), two of which may pertain to Stingray use.[87] The exception that is relevant to this paper is (5)(c), which reads: "any communication made through a *tracking device* consisting of an electronic or mechanical device which permits the tracking of the movement of a *person or object*."[88] As the memorandum points out, this language could be seen as exempting Stingrays from the eavesdropping warrant requirement, as Stingrays are often used as tracking devices.[89] However, the NYCLU still believes that this reason fails due to the New York Court of Appeals' 2009 decision in *People v. Weaver*,[90] which is discussed in Section III of this Comment. Finally, it is interesting to note that the memorandum does *not* think Stingrays fall under "primitive" pen register or trap and trace devices, despite the DOJ's statement to the contrary.[91] The NYCLU does not categorize Stingrays as such because they can do more than pen registers and trap and trace devices, such as "capture the unique manufacturer number and location information."[92] In

84. *Id.*

85. N.Y. PENAL LAW § 250.00(6) (2003) (emphasis added).

86. *Id.* § 250.00(5).

87. *Memorandum: Warrant Requirement*, *supra* note 35, at 2-3. *See* §§ 250.00(5)(a), (c).

88. § 250.00(5)(c) (emphasis added).

89. *Memorandum: Warrant Requirement*, *supra* note 35, at 3.

90. *Id.* ("Even if Stingrays were exempt as a tracking device, however, *People v. Weaver*, 12 N.Y.3d 433 (2009), as explained in Part II, requires law enforcement to obtain warrants for just such tracking uses.").

91. *Id. See Department of Justice Policy Guidance*, *supra* note 8, at 2 ("Moreover, cell-site simulators used by the Department must be configured as pen registers . . . ").

92. *Memorandum: Warrant Requirement*, *supra* note 35, at 3.

sum, the NYCLU advocates for a warrant requirement for Stingray use and has pointed to various applicable statutory provisions.[93]

Although the NYCLU cited federal and state constitutions as authority, it did not cite specific provisions besides a general right to be free from unreasonable searches and seizures.[94] An important provision to consider is Article I, Section 12 of the New York State Constitution.[95] The second paragraph reads:

> The right of the people to be secure against unreasonable interception of *telephone and telegraph communications* shall not be violated, and ex parte orders or *warrants shall issue* only upon oath or affirmation that there is a *reasonable ground* to believe that evidence of crime may be thus obtained, and identifying the particular means of communication, and particularly describing the person or persons whose communications are to be intercepted and the purposes thereof.[96]

A few things are worth noting. The first is the provision's reference to a telephone, considering the fact that this provision was adopted in 1938,[97] a time when telephones were not nearly as relevant as they are today. The second is the requisite burden of proof: reasonable belief.[98] While New York's Fourth Amendment counterpart adds greater protection to citizens, since the Fourth Amendment does not contain the paragraph quoted above,[99] it fails to make the necessary step in its protection. This provision would likely put an end to New York's unwarranted Stingray use if it required a warrant supported by probable cause, as opposed to an order or warrant

93. *Id.*
94. *Id.*
95. N.Y. CONST. art. I, § 12.
96. *Id.* (emphasis added).
97. *Id.*
98. *Id.*
99. *Id.* The Fourth Amendment, ratified in 1791, only protects "persons, houses, papers, and effects." U.S. CONST. amend. IV.

issued upon reasonable belief. Thus, although the 1938 provision is forward-looking in its paragraph about technology, it fails to provide an appropriate basis for holding New York state agencies accountable for unwarranted Stingray use. Let us consider how issues of privacy and location tracking have been decided in New York courts.

IV. Judicial Response: Burden of Privacy on the Citizen

Justice Harlan's concurrence in *Katz v. United States* (1961) established a framework for privacy, fully-equipped with a two-part subjective/objective analysis: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[100] This inquiry seems like the proper starting place in looking at judicial opinions regarding privacy, since the "*Katz* test" has been widely cited and is still followed today.

New York's unwarranted use of Stingrays may come as a bit of a surprise, considering its strict position on location tracking in *People v. Weaver*.[101] In that case, a police officer attached a GPS device to the defendant's car (unbeknownst to him).[102] The officer did *not* obtain a warrant before planting the device, which remained on the defendant's car for sixty-five days.[103] The record did not reveal why the officers wished to track the defendant, but the officers eventually charged and tried him with burglary.[104] The jury convicted him on both burglary counts.[105] The Appellate Division affirmed the defendant's conviction, holding that officers did not violate his Fourth Amendment right by tracking him without a warrant.[106] The Appellate Division also held that the defendant "had no greater right to relief under the State Constitution" and that he had a "reduced expectation or

100. Katz v. United States, 389 U.S. 347, 361 (1967).
101. *See generally* People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009).
102. *Id.* at 1195.
103. *Id.* at 1195-96.
104. *Id.* at 1196.
105. *Id.*
106. *Weaver*, 909 N.E.2d at 1196.

privacy in the exterior of his vehicle."[107]

The New York Court of Appeals disagreed. It began its analysis by distinguishing the United States Supreme Court's holding in *United States v. Knotts*.[108] In *Knotts*, officers placed a beeper on a five-gallon drum of chloroform to track the drum's location.[109] A car transported the drum across public roads before reaching its destination at the respondent's cabin.[110] The Court held that the defendant "undoubtedly had the traditional expectation of privacy within a dwelling place insofar as the cabin was concerned," but he had a lesser expectation of privacy concerning the "visual observation" of the car traveling on public roads and arriving at his cabin.[111] The Court also explained that the government made "limited use" of the beeper, ending its surveillance once the drum "ended its automotive journey" at the defendant's home.[112] The beeper aided law enforcement, who would not have been able investigate the whereabouts with a naked eye, and the Court stated that "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise."[113]

The *Weaver* court did not extend *Knotts'* rationale to the present case. The court held that the *only* similarity between the cases is that Mr. Weaver's car traveled on public roads, which anyone could have observed.[114] The court found significant the fact that the officers in *Knotts* used the "mere beeper" to track the chloroform drum for only one trip.[115] In contrast, the officers in this case tracked the defendant's car for sixty-five days.[116]

107. *Id.*

108. *See* United States v. Knotts, 460 U.S. 276 (1983). *See also* United States v. Skinner, 690 F.3d 772 (6th Cir. 2012) (holding that an individual did not retain a reasonable expectation of privacy in the location of his cellphone while traveling on a public road).

109. *Knotts*, 460 U.S. at 277.

110. *Id.*

111. *Id.* at 282.

112. *Id.* at 285.

113. *Id.*

114. *Weaver*, 909 N.E.2d at 1198-99 (citing *Knotts*, 460 U.S. at 281).

115. *Id.* at 1199.

116. *Id.* at 1195.

Since the United States Supreme Court had not yet decided "whether the use of GPS by the state for the purpose of criminal investigation constitute[d] a search under the Fourth Amendment,"[117] the court turned to New York's Constitution as a guide.[118] Since the court found that the officers infringed upon the defendant's expectation of privacy when they placed the GPS device on his vehicle and tracked his location, it thus held that the officers' activity constituted a "search" under the state's Constitution.[119]

Finally, the court expressed concern over the potential abuse of advanced tracking tools, noting that "the technology is rapidly improving so that any person or object, such as a car, may be tracked with uncanny accuracy to virtually any interior or exterior location, at any time and regardless of atmospheric conditions."[120] The court ultimately held that the officers should have obtained a warrant,[121] which preserves the valuable character of tracking technology while staying within "judicial oversight."[122] The court also noted that no exigent circumstance waived the warrant requirement.[123]

Three years later, the United States Supreme Court issued an opinion consistent with the majority's view in *Weaver*. In *United States v. Jones*, the Court held that placing a GPS device on a vehicle and tracking its movement constituted a "search" under the Fourth Amendment.[124] In that case, officers became suspicious that the defendant engaged in narcotics trafficking, so they applied to the United States District Court for the District of Columbia for a search warrant to install a GPS device on the defendant's car.[125] The court issued the warrant, but it authorized the officers to install the device *only*

117. *Id.* at 1202. The United States Supreme Court would later address this issue in *United States v. Jones*. *See infra* note 124.

118. *Weaver*, 909 N.E.2d at 1202.

119. *Id.* The court cited Article 1, Section 12 as the relevant Constitutional provision. *Id.*; *see* N.Y. CONST. art. I, § 12.

120. *Weaver*, 909 N.E.2d at 1199.

121. *Id.* at 1203.

122. *Id.*

123. *Id.* at 1201.

124. United States v. Jones, 132 S. Ct. 945, 949 (2012). *See also* U.S. CONST. amend. IV.

125. *Id.* at 948.

in that jurisdiction and "within [ten] days."[126]

The officers did not install the technology in the ten-day window and instead decided to install it while the car was parked in a "public parking lot" in Maryland.[127] The officers then used the GPS device to follow the car's movements for twenty-eight days.[128] The officers also had to replace the battery during that twenty-eight-day period, and they replaced it while the car was parked in a different parking lot in that state.[129] The tracking culminated in various drug charges filed against the defendant.[130]

Before trial, the defendant moved to suppress the evidence gathered through use of the tracking device.[131] The district court only granted the defendant's motion in regard to tracking the car while it was parked in a lot next to his home.[132] Regarding the rest of the data, the court cited *Knotts*' rationale that the defendant had "no reasonable expectation of privacy" while traveling on public roadways.[133] At trial, the jury convicted the defendant, and he received a life sentence.[134] On appeal, the D.C. Circuit reversed the defendant's conviction on the ground that the officers' use of the tracking device in Maryland, without a warrant, violated the defendant's Fourth Amendment right.[135]

The Supreme Court supported the D.C. Circuit's holding and offered independent reasons. The Court explained that the Fourth Amendment protects citizens from government trespass upon their "persons, houses, papers, and effects."[136] The Court also pointed to the government's *own* statement that the officers went beyond a plain observation of the defendant's vehicle when they attached the GPS device to the underbody of

126. *Id.*
127. *Id.*
128. *Id.*
129. *Jones*, 132 S. Ct. at 948.
130. *Id.*
131. *Id.*
132. *Id.*
133. *Id.* (citing *Knotts*, 460 U.S. at 281).
134. *Jones*, 132 S. Ct. at 949.
135. *Id.*
136. *Id.* at 951 (quoting U.S. CONST. amend. IV).

the car.[137] The Court thus concluded that "[b]y attaching the device to the Jeep, officers encroached on a protected area."[138] The Court affirmed the Court of Appeals' decision.[139]

In the meantime, lower New York courts have weighed in on expectations of privacy. As tracking technology has developed, so have the courts' views on who bears the burden in protecting privacy. Surprisingly, the New York courts do not follow the path taken by the *Weaver* and *Jones* courts. The first case in an important trilogy is *People v. Hall*. In that case, the defendant was indicted on murder and assault charges.[140] At trial, the defendant moved to "suppress historical cell site location information (CSLI) for calls made over his cell phone during the three-day period surrounding the shootings," but the court denied his motion.[141] The jury ultimately convicted the defendant of third-degree assault and second-degree criminal weapon possession.[142]

On appeal, the First Department affirmed the defendant's conviction.[143] The court also affirmed the lower court's denial of suppression on the ground that gathering the defendant's location information "did not violate the Fourth Amendment . . . because defendant had no reasonable expectation of privacy while traveling in public."[144] The court similarly found no constitutional argument under New York's Constitution.[145] The court also made a statutory argument, holding that 18 U.S.C § 2703(d) (2012) did not require the government to establish probable cause.[146] This statute, however, has since been held unconstitutional.[147]

137. *Jones*, 132 S. Ct. at 950-52 (questioning *Knotts*, 460 U.S. at 282).

138. *Jones*, 132 S. Ct. at 952.

139. *Id.* at 954.

140. People v. Hall, 926 N.Y.S.2d 514, 516 (App. Div. 2011).

141. *Id.*

142. *Id.*

143. *Id.* at 517.

144. *Id.* at 516. In fact, the First Department cited *Knotts* as authority for this contention. *Id.*

145. *Hall*, 926 N.Y.S.2d at 516.

146. *Id.*

147. *Id.* The Eleventh Circuit Court of Appeals deemed 18 U.S.C. § 2703 unconstitutional on the ground that the statute only required officers to have "reasonable ground" of suspicion (instead of probable cause) to obtain a warrant. United States v. Davis, 754 F.3d 1205, 1212-16 (11th Cir. 2014),

Finally, the First Department distinguished this case from *Weaver*.[148] The court considered the number of days involved in each tracking scheme; the detectives in *Weaver* tracked the defendant for sixty-five days, contrasted with "a mere 3 days" in this case.[149] It is interesting to note how the *Weaver* court contrasted its case with *Knotts* by also using the number of days, showing that the officers in *Weaver* tracked the defendant for a much longer span of time.[150] Thus, the *Weaver* court held that the unwarranted tracking violated the Fourth Amendment.[151] But in *Hall*, the court used *Weaver*'s strategy to reach a different outcome: since the officers in *Hall* only tracked the defendant's location for a few days, their activity did not rise to the level of a "protracted surveillance" in *Weaver*.[152] Although *Hall* addresses CSLI technology instead of Stingrays, it shows that New York courts might be returning to the *Knotts* framework of lessening a citizen's expectation of privacy in public places.

The second case in the trilogy is *People v. Moorer*, which introduces the idea that the burden of privacy might be on *the citizen*, as opposed to the government agency that wishes to gather the information and use it during investigations.[153] In that case, officers identified the defendant as a suspect in a homicide investigation.[154] They filed a request with Sprint, the defendant's service provider, to "ping" his phone and reveal its location.[155] Sprint, however, was unable to "ping" the defendant's phone because "it had been 'powered off.'"[156] The officers filed a second request, and this time, Sprint was able to

vacated, reh'g granted 573 F. App'x 925 (Mem) (2014). Although *Davis* has been vacated, pending rehearing *en banc*, there is nothing to indicate that § 2703 is valid law. To the contrary, the statute has pending legislation.

148. *Hall*, 926 N.Y.S.2d at 516.

149. *Id.* at 516-17 (citing *Weaver*, 909 N.E.2d at 1195).

150. *Weaver*, 909 N.E.2d at 1199 (citing *Knotts*, 460 U.S. at 279).

151. *Weaver*, 909 N.E.2d at 1202.

152. *Hall*, 926 N.Y.S.2d at 516-17.

153. *See generally* People v. Moorer, 959 N.Y.S.2d 868 (Monroe Cty. Ct. 2013).

154. *Id.* at 872.

155. *Id.* The officers claimed exigent circumstances because they were investigating a homicide and they believed the suspect was going to commit another homicide. *Id.*

156. *Id.*

pinpoint the phone's location to an eleven-meter radius.[157] The officers gained permission to enter and search the home where they suspected the phone to be and they found the phone in a backpack on the porch.[158] They ultimately charged the defendant with second-degree murder.[159]

Before trial, the defendant "moved to suppress all evidence obtained as a result of the 'pinging' of his cell phone . . . ."[160] During a suppression hearing, the defendant argued that the officers violated "both federal and state constitutional rights" when they conducted the searches without a warrant or court order.[161] Although the court denied the government's exigent circumstances argument, it ultimately held that the defendant's constitutional rights were *not* violated.[162]

The court focused its analysis on voluntary versus involuntary actions.[163] The court noted that location services in cell-phones are pre-installed "with the owner's consent or knowledge," as opposed to "physical[ly] install[ing]" a tracking device on a citizen's car without the person's permission.[164] The court made a sweeping policy argument about the increased use of cell-phones and privacy implications, stating:

> *public ignorance* about cell phone technology *can no longer be maintained* in this day and age—cell phones are *voluntarily carried* by their users and may be turned on or off at will. People are not so oblivious that they are not aware that cell phones purchased today come with GPS technology which can pinpoint the location of the phone at any given time so long as it is turned on and the GPS technology has not been deactivated or disabled . . . By a person's voluntary utilization, through GPS technology, of a cell

157. *Id.*
158. *Moorer*, 959 N.Y.S.2d at 872-73.
159. *Id.* at 871.
160. *Id.*
161. *Id.* at 874-75.
162. *Id.* at 875-81.
163. *Moorer*, 959 N.Y.S.2d at 881.
164. *Id.* at 878, 881.

> phone, a person necessarily *has no reasonable expectation of privacy* with respect to the phone's location—vis a vis the pinging—even though he maintains what may be a reasonable expectation of privacy in the content of his phone conversations.[165]

The court upheld the lower court's decision, holding that "pinging" the defendant's cell phone did not violate his rights.[166]

The court's language about the public's knowledge and use of cell phones represents a stark contrast from the DOJ's Sept. 3 policy. The DOJ policy does not say that citizens lessen their expectations of privacy by voluntarily carrying or using their cell phones. Rather, the DOJ explicitly shows that the *government* bears the burden of privacy because it now requires federal agencies to obtain warrants before cell-site simulators.[167] Thus, the federal agencies must prove why they want the location information. The *Hall* court, however, seems to say that *citizens* bear the burden of privacy and should already know that the government can track them if their phones are powered on. The court makes this point clear by saying citizens enjoy "no" expectation of privacy in this context, instead of "lessened." It can hardly be denied that many more citizens own technology than in past years, but the DOJ makes clear that it still intends to achieve a balance between security and privacy.

Following *Hall*'s lead, the third case in the trilogy continued the discussion of cell phone users and their expectations of privacy. In *People v. Wells*, the officers demonstrated exigent circumstances to "ping" the defendant's cell phone while investigating a shooting.[168] The court denied the defendant's suppression motion, and also commented on the developing debate about expectations of privacy:

> Finally, in this year, 2014, it can be said that cell

165. *Id.* (emphasis added).
166. *Id.*
167. *Justice Department Announces*, *supra* note 7.
168. People v. Wells, 991 N.Y.S.2d 743, 744 (N.Y. Sup. Ct. 2014).

> phone users, (including non-adult users) are *aware* of both the capacity for their phone to be located by GPS, and their ability to *avoid that function* by turning off their phone . . . it can no longer be said that one can reasonably expect that a cell phone that is turned on will have its location remain private . . . [it] is part of the package for cell phone users.[169]

Wells seems to be consistent with *Hall,* showing that the burden of privacy is on the citizen. The cases seem to imply that if someone does not want to be tracked, it is *up to them* to turn off their phones, *not* up to the government to prove why they need the information.

The purpose of this Comment is not to overstate the lower New York courts' holdings or extend their meaning beyond what was intended. The New York courts addressed the issue of "pinging" by cell-phone companies, *not* cell-site simulation conducted by the government. However, the underlying principles of security and privacy that can be pulled from these cases demonstrate the differing views of New York and the federal government. It is interesting that New York seemed to be *ahead* of the federal government in upholding citizens' privacy during location tracking. *Weaver*, decided in 2009, held that location tracking via GPS constituted a "search" under the Fourth Amendment.[170] The federal government, however, did not release its policy regarding Fourth Amendment concerns in location tracking via cell phones until 2015.[171]

The New York courts' exposure to location tracking, cell phones, and expectations of privacy did not end after the trilogy. In fact, it became *more specific*, involving Stingray technology and continued, unwarranted use of the technology. As noted earlier, the ACLU's map shows that New York state *and* local agencies use cell-site simulators.[172] The Erie County Sherriff's Office, however, wanted to keep its use of Stingray

169. *Id.* at 746 (emphasis added).
170. *Weaver*, 909 N.E.2d at 1202.
171. *Justice Department Announces*, *supra* note 7.
172. *Stingray Tracking Devices*, *supra* note 30.

technology under wraps.[173]

In July 2014, the NYCLU filed a public information request with the Erie County Sheriff's Office to obtain information about the office's use of "Stingray" technology.[174] After the office denied the request, the NYCLU brought an action in the New York Supreme Court, Erie County, in November 2014.[175] The NYCLU prevailed; the court ordered the office to release "purchase orders, a letter from the stingrays' manufacturer, a confidentiality agreement with [sic] between the Sheriff's Office and the FBI, a procedural manual and summary reports of instances in which the device was used."[176]

The NYCLU then released its findings, which showed that the office used the technology "at least 47 times between May 1, 2010 and October 3, 2014, including assisting other law enforcement departments like the Monroe County Sheriff's Office."[177] In addition, the office obtained a court order only one time.[178] Finally, the NYCLU's records revealed that the confidentiality agreement with the FBI required the office to "maintain almost secrecy over stingray records" and "dismiss criminal prosecutions [at times] rather than risk compromising the secrecy of how stingrays are used."[179]

The New York Supreme Court's order requiring the office to release records shows a possible shift in New York's stance on privacy. The decision shows a lack of tolerance for unwarranted Stingray use in New York. New York courts may rethink earlier ideas of privacy that stemmed from cases like *Moorer* and *Hall*. Since this appears to be the first time a New York court dealt with Stingray technology, maybe the courts will decide future cases in accordance with the Erie County

173. *See Erie County Sheriff Records Reveal Invasive Use of "Stingray" Technology*, N.Y. CIVIL LIBERTIES UNION (Apr. 7, 2015), http://www.nyclu.org/news/erie-county-sheriff-records-reveal-invasive-use-of-stingray-technology [hereinafter *Erie County Sheriff Records*].

174. *In re* N.Y. Civil Liberties Union v. Erie Cty. Sheriff's Office, No. 2014/000206, 2015 WL 1295966, at *1 (N.Y. Sup. Ct. 2015).

175. *Id.*

176. *Erie County Sheriff Records*, *supra* note 173.

177. *Id.*

178. *Id.*

179. *Id.*

case.

Recently, in a case of first impression in Maryland, the Court of Special Appeals considered whether "a cell phone—a piece of technology so ubiquitous as to be on the person of practically every citizen—may be transformed into a real-time tracking device by the government without a warrant."[180] The court held that it cannot, stating that the "people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement, and . . . that people have an objectively reasonable expectation of privacy in real-time cell phone location information."[181] Since the state's use of cell-site simulator technology invoked the Fourth Amendment, the court required more than a simple court order; it required a warrant or "a specialized order that [includes] a particularized showing of probable cause . . . . "[182]

It is true that the United States Supreme Court has yet to decide whether Stingray technology implicates Fourth Amendment concerns.[183] However, the issue recently reached a federal district court in Manhattan, where the court invalidated the search of a Washington Heights apartment after officers seized drugs they discovered through unwarranted cell-site simulator use.[184] This was a landmark ruling, as a federal judge had never suppressed such evidence before.[185] With the issue gaining attention in the lower federal courts, Supreme Court review may not be as far away as before. At the very least, we *do* know how the Supreme Court will handle searches of a cell phone's contents in the future.[186]

180. State v. Andrews, 134 A.3d 324, 326 (Md. Ct. Spec. App. 2016).

181. *Id.*

182. *Id.* at 358.

183. Timothy Williams, *Covert Electronic Surveillance Prompts Calls for Transparency*, N.Y. TIMES (Sept. 28, 2015), http://www.nytimes.com/2015/09/29/us/stingray-covert-electronic-surveillance-prompts-calls-for-transparency.html?_r=0.

184. Benjamin Weiser, *D.E.A. Needed Warrant to Track Suspect's Phone, Judge Says*, N.Y. TIMES (July 12, 2016), http://www.nytimes.com/2016/07/13/nyregion/dea-needed-warrant-to-track-suspects-phone-judge-says.html.

185. *Id.*

186. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014) ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even

Through the recent cell-site simulator case in Maryland, we also see the state courts analyzing traditional Fourth Amendment concepts of searches, probable cause, and warrants, applying them to modern day location-tracking. But New York should not wait to hear from the Court, or even its own courts; it should invoke its legislative authority and require warrants based on probable cause.

IV. Legislative Response: Three Pending Bills

State and federal legislators are responding to the public's privacy concerns in unwarranted use of Stingrays. Two bills have been proposed in New York that would change the way its state and local agencies use cell-site simulators. A federal bill has also been proposed that would require *all* state and local agencies to obtain warrants based on probable cause before using the technology.

The first bill is New York Senate Bill S4914A, sponsored by New York Senator Michael Ranzenhofer.[187] The bill was proposed on April 23, 2015 and is currently in the committee.[188] The bill seeks to amend New York's Criminal Procedure Law section 705 by adding a seventh definition.[189] A definition of "mobile phone surveillance device or system" would include "technology that identifies, tracks, or locates cellular devices by forcing each compatible cellular device in a given area to disconnect from its service provider cell site and establish a new connection with the device by mimicking a wireless cell tower."[190] This bill does *not* rise to the level of the DOJ's warrant requirement, but instead proposes a court order requirement.[191] The officer would only need to demonstrate "reasonable suspicion that a designated crime has been, is being, or is about to be committed . . ." to obtain permission to

when a cell phone is seized incident to arrest."). The *Riley* Court cites *Jones* and references a cell phone's ability to "reconstruct someone's specific movements down to the minute," *id.* at 2490, but the Court does not address location-tracking in depth.

187. S.B. 4914A, 2015-2016, Reg. Sess. (N.Y. 2015).

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

track a person's location.[192] Considering the DOJ's and other states' warrant requirements, this proposed bill would still keep New York courts behind, as it appears from the NYPD's statement that it *does* seek court orders before using the technology.[193]

The second proposed bill, however, rises to the appropriate level. New York Senate Bill 8055, introduced on June 5, 2015, seeks to require officers to obtain a warrant based on probable cause before using a cell site simulator to reveal a person's location.[194] The bill seeks to amend the definitions under New York's eavesdropping law by adding the words "includes the use of a cell site simulator device" after the definition of "eavesdropping."[195] The bill also intends to add a definition for "cell site simulator device," which would mean "a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (A) identifying, locations, or tracking the movements of a communications device. . . ."[196] Finally, the bill wants to make sure that cell-site simulators fit under the state's eavesdropping laws so that they require a warrant supported by probable cause; the bill seeks to amend section 700.20(ii) (eavesdropping warrant application) by adding "to the extent known for a warrant authorizing use of a cell site simulator device."[197]

In November 2015, United States Representative Jason Chaffetz introduced the "Stingray Privacy Act of 2015," which would require *any* "governmental entity" to obtain a warrant before using a cell-site simulator.[198] His proposed bill is not limited to federal agencies.[199] The bill does not set out a probable cause requirement, but it specifies the way in which cell-site simulators should be used.[200] For example, the bill requires that no evidence obtained through a cell-site simulator

192. S.B. 4914A.

193. Letter from Richard Mantellino, *supra* note 68.

194. Assemb. 8055, 2015-2016, Reg. Sess. (N.Y. 2015), http://legislation.nysenate.gov/pdf/bills/2015/A8055.

195. *Id.*

196. *Id.*

197. *Id.*

198. Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015).

199. *Id.*

200. *Id.*

can be used during a proceeding, except if the agency obtains a warrant, conducts electronic surveillance, or uses it during an emergency.[201] It is interesting to note that it specifically addresses national security,[202] which seems to be at the forefront of issues facing the federal government.

V. Conclusion: New York Should Require a Warrant

The body of research surrounding cell-site simulators indicates that the devices are another piece of technology that our laws have not quite caught up to yet, similar to cell phone capabilities and social networking sites. But this does not mean that we should accept the *status quo*. For one, the DOJ shows that it is paying attention to citizens' desire for privacy, while at the same time trying to keep these same citizens safe. Thus, I believe that New York should follow suit and adopt a warrant requirement supported by probable cause.

Although the results in the lower New York courts demonstrate otherwise, I argue that the burden should be on the government to show why it needs to invade citizens' privacy. The Erie County revelation seemed to shock New York citizens, which shows that it is the appropriate moment for the state to establish an official Stingray policy with a probable cause requirement. Other states have adopted new policies or clarified their policies even before the DOJ did. As the DOJ notes, there are ways to balance privacy and national security. It is completely understandable that there are exceptions to warrant requirements, especially in the wake of violence within this country and overseas. But, absent exigency or emergency, both the federal and state governments should obtain warrants supported by probable cause before they employ these high-tech devices. New York should be no different.

201. *Id.*
202. *Id.*